Patent Claims

1. A method for secure data transmission between a first subscriber (T1) and second subscribers (T2), particularly between a tachograph (51) in a commercial vehicle and memory cards (50) having at least one respective data store, where the first subscriber (T1) has a memory (6, 22) which stores a particular number of entries (31-35), each comprising identifiers (4) and associated security certificates (Cert) from second subscribers (T2) with a detection time (53) for the security certificate (Cert), which method involves the first subscriber (T1) fetching an identifier (4) from the second subscriber (T2), the first subscriber (T1) comparing this identifier (4) with the identifiers (4) stored in the memory (6, 22), a matching identifier (4) stored in the memory (6, 22) prompting the security certificate (Cert) associated with this identifier (4) to be the basis for a subsequent data transmission, and the detection time (53) for the security certificate (Cert) being updated to a current system time, no matching identifier (4) stored in the memory (6, 22) prompting the first subscriber (T1) to perform security certificate verification with the second subscriber (T2) and, in the event of verification, storing an entry (31-35) corresponding to the verified security certificate (Cert) with the current detection time (53) in the memory (6, 22), with the entry (31-35) with the oldest detection date being replaced by this new entry (31-35) if the particular number of entries (31-35) has already been reached.

2. The method as claimed in claim 1, characterized in that the identifier (4) is a public key from an RSA method from the second subscriber (T2).

3. The method as claimed in claim 1, characterized in that a subsequent data transmission is effected in TDES-encrypted

form, with verification of the security certificates (Cert) being followed by both subscribers (T1, T2) sending a random number (RND) in encrypted form to the other subscriber (T1, T2) and both subscribers (T1, T2) independently of one another each using the two random numbers (RND) to determine a common key (80) for data transmission using the same algorithm.

4. The method as claimed in claim 1, characterized in that the verification of the security certificate (Cert) from the first subscriber (T1) by the second subscriber (T2) and vice versa comprises the following n steps:
in a first step the second subscriber (T2) sends the first subscriber (T1) a first security certificate (Cert.Lev.1), which the second subscriber (T2) subjects to verification using a first public key and in so doing ascertains a second public key,
if the verification results in authenticity then the first step is repeated (n-1) times using a further transmitted security certificate (Cert.Lev.1, 2) and the second public key ascertained in the previous step instead of the first public key, with a new second public key and a verification result always being obtained.

5. The method as claimed in claim 1, characterized in that n = 3.